



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 03 août 2004
N° CERTA-2004-AVI-261

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des navigateurs Netscape et Mozilla

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-261>

Gestion du document

Référence	CERTA-2004-AVI-261
Titre	Vulnérabilité des navigateurs Netscape et Mozilla
Date de la première version	03 août 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité de iDefense du 02 août 2004
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

- Mozilla versions 1.6 et antérieures ;
- Netscape versions 7.x.

3 Résumé

Une vulnérabilité des navigateurs Netscape et Mozilla permet à un utilisateur distant d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Une vulnérabilité a été découverte dans la gestion du protocole SOAP (Simple Object Access Protocol) par les navigateurs Netscape et Mozilla.

Un utilisateur distant mal intentionné peut exploiter cette vulnérabilité par le biais d'une page HTML habilement forgée pour exécuter du code arbitraire.

5 Contournement provisoire

Désactiver le javascript.

6 Solution

La version 1.7.1 de Mozilla corrige cette vulnérabilité (cf. section Documentation).

Netscape n'a pas fourni d'information concernant cette vulnérabilité.

7 Documentation

- Site web de la fondation Mozilla :
<http://www.mozilla.org>
- Bulletin de sécurité de iDefense du 02 août 2004 :
<http://www.iddefense.com/application/poi/display?id=117>
- Référence CVE CAN-2004-0722 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0722>

Gestion détaillée du document

03 août 2004 version initiale.